EXHIBIT B-5

Cobert testifies about the agency's relationship with the Inspector General before the Committee on May 13, 2016

It is also noteworthy that Cobert added cyber talent to the agency.[1025] McFarland attributed improvement in the OCIO-OIG relationship to one of these staff additions.[1026] On November 4, 2015, Cobert announced the addition of Clifton ("Clif") Triplett to the OPM cyber team.[1027] Reporting directly to Cobert, Triplett is tasked with advancing the state of enterprise architecture and cybersecurity, including information technology investments, capabilities, and services.[1028] Working alongside OPM's CIO—currently Acting CIO Lisa Schlosser[1029]—Triplett supports the ongoing response to the 2015 incidents, completing the development of OPM's plan to mitigate future incidents, and recommends further improvements to best secure OPM's IT architecture.[1030] Triplett has thirty years of broad executive management experience, including work on Top Secret and other advanced technologies in the protection and defense of the U.S. Nuclear Command and Control Systems.[1031]

Vint's draft testimony stated that Triplett helped to mend internal relationships. Vint's testimony stated:

> We believe that the new Senior Cyber and Information Technology Advisor, Clifton N. Triplett, has helped facilitate this improved

[1025] U.S. Office of Pers. Mgmt., Press Release, *OPM Director Announces Key New Cyber Advisor* (Nov. 4, 2015), https://www.opm.gov/news/releases/2015/11/opm-director-announces-key-new-cyber-advisor-2/.
[1026] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt. at 5) (hearing cancelled).
[1027] U.S. Office of Pers. Mgmt., Press Release, *OPM Director Announces Key New Cyber Advisor* (Nov. 4, 2015), https://www.opm.gov/news/releases/2015/11/opm-director-announces-key-new-cyber-advisor-2/.
[1028] *Id.*
[1029] U.S. Office of Pers. Mgmt., *Lisa Schlosser: Acting Chief Information Officer* (May 17, 2016), https://www.opm.gov/about-us/our-people-organization/senior-staff-bios/lisa-schlosser/.
[1030] U.S. Office of Pers. Mgmt., Press Release, *OPM Director Announces Key New Cyber Advisor* (Nov. 4, 2015), https://www.opm.gov/news/releases/2015/11/opm-director-announces-key-new-cyber-advisor-2/.
[1031] *Id.*

> relationship as well as create additional avenues of communication between the OIG and the agency's IT staff. It appears that Triplett's role is to provide high level advice to assist the Acting Director in developing a strategy to address the multitude of IT challenges facing OPM. I and other senior OIG officials meet with Triplett on almost a weekly basis. From what we understand, he agrees with the OIG that the agency needs to have a comprehensive plan moving forward that would include a short-term plan to address the needs of OPM's critical IT systems, as well as a long-term plan for the implementation of OPM's agency-wide Infrastructure Improvement Project."[1032]

Cobert testified that the relationship had improved from her perspective. In response to a question from Rep. Mark Meadows (R-NC) at a hearing on May 13, 2016, Cobert testified:

> We have been working across the agency to strengthen our effectiveness of our dialogue with the CIO and I believe we've made real progress in a number of different areas. We've set up a cadence of regular communications at my level with the Inspector General, currently Acting Inspector General. On a bi-weekly basis, we meet and get an overview of the issues. We have specific working teams that meet on a periodic basis as well - both around the CIO, around procurement, we've set up that same kind of mechanism on the stand-up of the NBIB given the oversight issues there and wanting to make sure we get those right. So I think we've made considerable progress in terms of the dialogue, the clarity of the communications. We welcome their input on what we could be doing as better. As we welcome input from our colleagues here and elsewhere."[1033]

Cobert characterized the relationship as "much improved."[1034] While the OIG reported being "pleased" that communications have improved, the office was "still concerned about OPM's overall IT strategy."[1035] Vint committed that the OIG would "continue to monitor the OCIO's activities and work with them to ensure that actions discussed at meetings are, in fact, implemented – and implemented in accordance with proposed timelines."[1036]

[1032] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.at 5) (hearing cancelled).

[1033] Incorporating Social Media into Federal Background Investigations: Hearing Before Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec. of the H. Comm. on Oversight & Government Reform, 114th Cong. at 1:12.35 (May 13, 2016), https://oversight.house.gov/hearing/incorporating-social-media-federal-background-investigations/.

[1034] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.at 5) (hearing cancelled).

[1035] *Id.*

[1036] *OPM Data Breaches: Part III Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt. at 5) (hearing cancelled).

Summary of OIG and OCIO relationship

Federal watchdogs play a critical role in the federal government, one that is statutorily-driven by the Inspector General Act of 1978. Despite the key role IGs play, the relationship between OPM OIG and its OCIO became strained while Katherine Archuleta served as Director and Donna Seymour as CIO. Despite serious concerns raised by the OIG in July 2015, and despite concerns raised by Congress about Seymour,[1037] Acting Director Cobert maintained support for Seymour, allowing her to hold a leadership role until her retirement on February 22, 2016.[1038] Overall however, the OCIO's relationship with the IG steadily improved under Acting Director Cobert's leadership and today is reported by both entities to be without conflict.[1039] The future effectiveness of the agency's information technology and security efforts will depend on a strong relationship between these two entities moving forward.

[1037] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Interim Dir., Office of Pers. Mgmt (Aug. 6, 2015); Letter from 18 Members of Congress, to Barack Obama, President, United States (June 26, 2015) (raising concerns about OPM Director Katherine Archuleta and OPM Chief Information Officer Donna Seymour).

[1038] Aaron Boyd, *OPM CIO Seymour Resigns Days Before Oversight Hearing*, FEDERAL TIMES, Feb. 22, 2016, *available at:* http://www.federaltimes.com/story/government/it/cio/2016/02/22/opm-cio-seymour-resigns/80766440/; Billy Mitchell, *Office of Personnel Management CIO Donna Seymour Retires*, FEDSCOOP, Feb. 22, 2016, available at: http://fedscoop.com/opm-cio-seymour-retires; Ian Smith, *OPM CIO Donna Seymour Resigns*, FEDSMITH, Feb. 22, 2016, available at: http://www.fedsmith.com/2016/02/22/opm-cio-donna-seymour-resigns/.

[1039] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.at 5) (hearing cancelled); *Incorporating Social Media into Federal Background Investigations: Hearing Before Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (May 13, 2016).

Chapter 8: The IT Infrastructure Improvement Project: Key Weaknesses in OPM's Contracting Approach

On March 20, 2014, DHS/USCERT informed OPM that a third party had exfiltrated data from OPM's network.[1040] In response to this discovery and after identifying serious vulnerabilities in the OPM network, the agency initiated the IT Infrastructure Improvement project. Seymour testified before the Committee that this project began as a consequence of the March 2014 cyber incident.[1041]

This project was intended to quickly secure OPM's legacy IT environment with the urgent procurement of security tools (Tactical, phase 1) and to fully overhaul OPM's IT infrastructure with a new IT environment that included security controls (building the Shell, phase 2). After building the new IT environment (the Shell), the plan was to migrate OPM's entire IT infrastructure into the new IT environment (Migration, phase 3) and then decommission legacy IT hardware and systems (Clean Up, phase 4). In June 2014, OPM made a sole source award to Imperatis to execute this project.[1042]

As of May 2016, multiple security tools have been purchased—some with only limited due diligence—to secure OPM's legacy IT environment, and a new IT environment has been built (the Shell). After the agency paid a contractor over $45 million for the Tactical and Shell phases, the June 2014 contract was terminated in May 2016 and, as the IG predicted, OPM had two IT environments (legacy and the new Shell) to maintain.[1043] Meanwhile, OPM continues to address concerns first raised by the IG in June 2015 about OPM's contracting approach. Specifically, the IG expressed concern that this investment was made with limited consideration of alternatives and without a full understanding of the scope of existing IT assets and potential costs to execute the entire project.[1044]

The taxpayers' return on this investment is now further in question after the creation of the National Background Investigations Bureau (NBIB), "which will absorb [OPM's] existing Federal Investigative Services (FIS)," and now that the Department of Defense "will assume the responsibility for the design, development, security and operation of the background investigations IT systems for the NBIB."[1045] These developments present a funding challenge for this project because OPM initially planned to rely on funds from OPM's revolving fund,

[1040] June 2014 OPM Incident Report at HOGR0818-001233.
[1041] *OPM Data Breach: Hearing Before the H. Comm. On Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Mgmt.).
[1042] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015).
[1043] OIG Flash Audit Alert (June 17, 2015) at 5 (stating "in this scenario, the agency would be forced to indefinitely support multiple data centers, further stretching already inadequate resources possibly making both environments less secure, and increasing costs to taxpayers."); Email from Imperatis to H. Comm. on Oversight & Gov't Reform Majority Staff (June 7, 2016) (confirming total paid to Imperatis from June 16, 2014 to May 6, 2016 is $45.1 million) (on file with the Committee).
[1044] OIG Flash Audit Alert (June 17, 2015).
[1045] White House, Press Release, *The Way Forward for Federal Background Investigations* (Jan. 22, 2016), https://www.whitehouse.gov/blog/2016/01/22/way-forward-federal-background-investigations.

which is largely derived from background investigation fees OPM collected from other agencies.[1046]

The documents and testimony show OPM's IT Infrastructure project would have benefited from more robust communications with the IG, particularly in responding to cybersecurity incidents. Former OPM CIO Donna Seymour testified she was not aware of a requirement "to notify the IG of every project that we take on."[1047] Given the significant funding for the IT Infrastructure project, which initially had an overall estimated cost of $93 million, the agency-wide nature of this project, and the fact that this project was launched as a consequence of the 2014 data breach, OPM should have involved the OIG so that the expertise of his office could help the agency deter problems before they arose. Because agency did not communicate with the IG on the front end, OPM found itself spending significant time and effort responding to IG concerns after the fact. In this case, the IG found out about the project a year after it was launched.[1048] Shortly thereafter, the IG issued a Flash Audit Alert that contained serious concerns.[1049] The IG and OPM continue to have discussions about these concerns.

The documents and testimony show there should be pre-established contract vehicles for cyber incident response and related services. Instead of issuing a sole source contract to facilitate the procurement of security tools to secure a compromised IT network, in the midst of an emergency situation and without the benefit of competition, there should have been a government-wide contract vehicle already established to fulfill this need. Just as emergency preparedness officials learned the value of establishing contract vehicles to support emergency response to natural disasters prior to such disasters after Hurricane Katrina, so too should similar resources be established for responding to cybersecurity emergencies.[1050]

The state of OPM's IT legacy environment leading up to the 2014 and 2015 breaches illustrates the pressing need for federal agencies to modernize legacy IT in order to mitigate the cybersecurity threat inherent in unsupported, end of life IT systems and applications. The GAO recently observed that in cases where vendors no longer support hardware or software this can create security vulnerabilities and additional costs.[1051] In testimony before the Committee, then-OPM CIO Seymour admitted the vulnerability of OPM's legacy. She stated:

[1046] *OPM Data Breach: Part III: Hearing Before the H. Comm. on Oversight &Gov't Reform* (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (hearing cancelled).
[1047] *OPM Data Breach: Part II Hearing Before the H. Comm. on Oversight &Gov't Reform*, 114th Cong. (June 24, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[1048] U.S. Office of Personnel Management, Office of Inspector Gen., *Background Information: OPM Infrastructure Overhaul and Migration Project* (June 17, 2015) (on file with the Committee).
[1049] OIG Flash Audit Alert (June 17, 2015).
[1050] In October 2015, OMB released a Cybersecurity Strategy and Implementation Plan (CSIP) that reported an effort to establish a contract vehicle in order to develop a capability to deploy incident response services that could be used by agencies on an expedited basis. Memorandum from Shaun Donovan, Dir., and Tony Scott, Fed. Chief Info. Officer, Office of Mgmt. & Budget, Exec. Office of the President, to Agency Heads, M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (Oct. 30, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.
[1051] Gov't Accountability Office, GAO-16-468, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems* 27(May 2016).

> OPM has procured the tools, both for encryption of its databases, and we are in the process of applying those tools within our environment. But there are some of our legacy systems that may not be capable of accepting those types of encryption in the environment that they exist in today.[1052]

Further, in making the case for updating aspects of OPM's legacy IT environment in the context of this contract, Imperatis said certain servers could no longer be patched and hardware had to be replaced in order to mitigate the risk of catastrophic failure since the current hardware was "woefully out of service."[1053] The need to modernize is clear, however, the modernization of such systems should not be done through a sole source contract in an emergency situation and without a full assessment of alternatives and understanding of the scope and cost of such an effort.

The IG Issues a Flash Audit Alert and Interim Reports on the IT Infrastructure Project

On June 17, 2015, the IG issued a Flash Audit Alert to then-Director Katherine Archuleta on the sole source IT contract to secure and update OPM's legacy IT infrastructure.[1054] The IG raised serious concerns about this project and "identified substantial issues requiring immediate action" and urged the CIO to "immediately begin taking steps to address these concerns."[1055] McFarland wrote:

> [O]ur primary concern is that the OCIO has not followed the U.S. Office of Management and Budget (OMB) requirements and project management best practices. . . the OCIO has initiated this project without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and costs of the effort required to migrate it to the new environment.[1056]

McFarland also expressed concerns "with the nontraditional Government procurement vehicle that was used to secure a sole-source contract with a vendor to manage the infrastructure overhaul."[1057]

These two themes (lack of project management and the sole source contracting approach) have been present throughout the IG's oversight of this project with varying levels of cooperation from OPM. Over time and more recently, OPM officials have become more responsive to the IG's concerns, particularly as new OPM leadership was put in place.

[1052] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Mgmt.).
[1053] Email from [redacted] Imperatis to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (July 31, 2014, 3:18 p.m.), Attach. 9a at 001163 (Imperatis Production: Sept. 1, 2015); Email from [redacted] Dir. Stragetic Growth, Imperatis to [redacted] U.S. Office of Pers. Mgmt. (Mar. 20, 2015, 3:12 p.m.), Attach 9a at 001170 (Imperatis Production: Sept. 1, 2015).
[1054] OIG Flash Audit Alert (June 17, 2015).
[1055] *Id.* at 1.
[1056] *Id.*
[1057] *Id.*

With respect to the project management concerns, the IG observed at the time that OPM had not "identified the full scope and cost of this project" and had not prepared a Major IT Business case document (which is an OMB requirement for major IT investments).[1058] As a result of the inadequate project management, the IG found "a high risk that this Project will fail to meet the objectives of providing a secure operating environment for OPM systems and applications."[1059] The IG recommended that OPM complete the Major IT Business case document as part of the FY 2017 budget process.[1060]

The IG predicted the failure to plan and understand the full scope of the project also would introduce schedule and cost risks.[1061] For example, OPM did not have a complete IT inventory of existing applications and systems for migration and redesign.[1062] In addition, the cost estimate at the time for the Tactical and Shell phases was approximately $93 million and did not include the cost of migrating legacy applications to the new environment.[1063] The source of funding was also unclear. The IG stated: "when we asked about the funding for the Migration phase, we were told, in essence, that OPM would find the money somehow, and that program offices would be required to fund the migration of applications that they own from their existing budgets."[1064]

With respect to the sole source contract award issue, the IG questioned the use of a sole source contract for all four phases of the network infrastructure improvement project.[1065] The IG acknowledged that the sole source approach may have been appropriate for the first Tactical phase of the project given the immediate need to secure the legacy IT environment.[1066] The IG did not agree, however, that it was appropriate to use this sole source contract for all four phases of the project. Chairman Chaffetz raised those concerns in a June 24, 2015 hearing. He stated: ". . . when it is a sole-source contract, it does beg a lot of questions."[1067]

The IG recommended against using a sole-source contract for all four phases of this project because "without submitting this project to an open competition, OPM has no benchmark to evaluate whether the costs charged by the sole-source vendor are reasonable and appropriate."[1068]

On June 22, 2015, former Director Katherine Archuleta responded to the IG's Flash Audit Alert and generally disagreed with IG's concerns.[1069] She argued that a business case was

---

[1058] OIG Flash Audit Alert (June 17, 2015) at 2.
[1059] *Id.*
[1060] *Id.* at 5.
[1061] *Id.* at 2.
[1062] *Id.* at 3.
[1063] *Id.*
[1064] *Id.*
[1065] *Id.* at 5-6.
[1066] *Id.* at 5.
[1067] *Hearing on OPM Data Breach: Part II* (Statement of Chairman Chaffetz).
[1068] OIG Flash Audit Alert (June 17, 2015) at 6.
[1069] Memorandum from Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt., to Patrick McFarland, Inspector Gen. U.S. Office of Pers. Mgmt., *Response to Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure*

not necessary and would take too long. With respect to the concern that OPM lacked a full understanding of the size, scope, and cost, OPM said: "OPM and the OCIO have always been very clear that the undertaking includes factors and costs that will be understood more clearly as the Project proceeds"—essentially, "we will figure it out as we go."[1070]

OPM also disputed the IG's characterization of the contract as a sole-source award covering all four phases of the IT Infrastructure Improvement project and took the opportunity to state "the contract for the Migration and Cleanup phases of the infrastructure improvement project have not yet been awarded."[1071]

The IG's Concerns Continued through the Fall of 2015

On September 3, 2015, the OIG released an Interim Status Report on the Flash Audit Alert.[1072] The OIG's Interim Status Report acknowledged developments related to this effort that in the IG's view emphasized the need for a "disciplined project management approach."[1073] Such developments included former Director Archuleta's resignation, Senate appropriators' rejection of OPM's $37 million funding request for accelerated migration of IT systems in July 2015, and the fact that OPM had identified "serious security vulnerabilities" in several IT systems, including e-QIP (which is the electronic questionnaire systems for background investigations).[1074]

In the Interim Status Report, the IG reiterated the recommendations in the original Flash Audit Alert and pointed out that OPM has "not yet determined the full scope and overall costs of the Project" and without completing a Major IT Business Case proposal for the Project, the IG concluded "there is a high risk of project failure."[1075] Further, the IG said the sole source award for all four phases and the original justification for making such an award "violate[d] federal acquisition regulations" because "*any* involvement that is not required to correct the urgent and compelling circumstances" would not be justified under the urgent and compelling exception authorizing certain sole source contracts.[1076]

IG Reports Progress in Responding to Concerns, but Challenges Remain as of May 2016

Almost one year after the OPM IG issued a Flash Audit Alert on OPM's IT Infrastructure Improvement project, Acting IG Norbert Vint issued the Second Interim Report on this project in

---

Improvement Project (Report No. 4A-CI-00-15-055) (June 22, 2015)[hereinafter Archuleta Response to IG Flash Audit Alert].

[1070] Archuleta Response to OIG Flash Audit Alert at 3.

[1071] *Id.* at 2.

[1072] Office of the Inspector Gen., U.S. Office of Personnel Mgmt., Report No. 4A-CI-00-15-055, *Interim Status Report on OPM's Responses to the Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Project* (Sept. 3, 2015) [hereinafter OIG Interim Status Report (Sept. 3, 2015)].

[1073] *Id.* at 2.

[1074] *Id.* at 1-2.

[1075] *Id.* at 2, 5.

[1076] *Id.* at 7 (emphasis in original) (citing 48 C.F.R. 6.302); 41 U.S.C. 3304(a)(2).

May 2016.[1077] The Acting IG reported some progress with OPM's submission of a major IT Business Case during the FY 2017 budget process, but the Acting IG also said there were lingering overall concerns about the project related to the insufficient capital planning process and unsubstantiated lifecycle cost estimates.[1078] The Acting IG made two recommendations: (1) OPM should conduct an Analysis of Alternatives (AoA) to determine whether the Shell (which is now known as Infrastructure as a Service or IaaS) is the best approach to modernizing the IT environment given changes in the internal and external environments; and (2) OPM should continue to leverage the application profile scoring framework developed by OPM in order to develop reliable cost estimates for modernization and migration activities.[1079]

In May 2016, the Acting IG reported that OPM had submitted a Business Case for this project (as part of the FY 2017 budget process) in response to the IG's prior recommendation. However, after reviewing the document the Acting IG said the document was insufficient because OPM did not perform capital planning activities, such as a performing an AoA to the Shell/Iaas and had not developed a solid cost estimate for modernization and migration.[1080] The Acting IG said OPM still had not determined the full scope of the project, but there had been some improvement in developing an inventory of legacy systems and estimating costs to modernize these systems.[1081]

In addition, the Acting IG identified a new complication to funding the IT Infrastructure Improvement project. Specifically, the decision to create the NBIB and designate the Department of Defense as responsible for the IT systems to support the background investigation process altered the potential funding options. OPM had planned to rely on its revolving fund, which is primarily funded through revenues from the background investigation process, to support the IT Infrastructure Improvement project.[1082] With the creation of the NBIB, the background investigation processing function will no longer be part of the Shell/Iaas. Consequently, this funding source is no longer available.[1083]

The Acting IG concluded that while it was not too late for OPM to complete the capitol planning activities (which should have been done prior to project initiation), the IG remains concerned that "there is a very high risk that the project will fail to meet its stated objectives of delivering a more secure environment at a lower cost."[1084]

On April 22, 2016, OPM's Acting CIO Lisa Schlosser offered OPM's response to the Second Interim Report and said OPM's OCIO "appreciates the detailed analysis and feedback provided in the report and generally concurs with the recommendations."[1085] The OCIO

[1077] Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-16-037, *Second Interim Status Report on the U.S. Office of Personnel Mgmt's Infrastructure Improvement Project – Major IT Business Case* (May 18, 2016) [hereinafter OIG Second Interim Status Report on Infrastructure Improvement Project (May 18, 2016)].
[1078] *Id.*
[1079] *Id.* at 5, 8.
[1080] *Id.* at 4.
[1081] *Id.* at 8.
[1082] *Id.* at 5.
[1083] *Id.*
[1084] *Id.* at 5.
[1085] U.S. Office of Personnel Mgmt. Acting Chief Info. Officer Lisa Schlosser *Response* (Apr. 22, 2016) to Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-16-037, *Second Interim Status Report on the U.S.*

Response then proceeded to provide details on ongoing efforts and planned next steps to address the IG recommendations. For example, the Acting CIO said, OPM has "engaged in on-going efforts to inventory IT systems and identify plans to mitigate, migrate, or modernize these systems."[1086] Further, OPM agreed that this project would benefit from a more rigorous lifecycle cost estimating process and pointed to a plan to use an application profile framework (developed by OPM's Senior Cybersecurity and IT Advisor) to inform lifecycle cost estimates for IT modernization.[1087]

In sum, OPM has come a long way from the state of affairs in June 2015 when the IG released the Flash Audit Alert on the IT Infrastructure Improvement project. Today, OPM is currently working cooperatively with the IG to mitigate concerns raised by the IG. The agency appears to be making progress on completing basic capitol planning activities that should have been completed prior to the launch of this project and these efforts should be acknowledged. However, the IG continues to have concerns about this project and unfortunately some of the risks identified early on by the IG seem to have played out during the course of the Imperatis contract.

The Story of OPM's IT Infrastructure Improvement Project and the Sole Source Contract

Over the past two years, OPM has made progress toward securing OPM's legacy IT environment and building a new IT environment, but there were significant concerns raised by IG about the IT Infrastructure contract that were validated and expanded upon based on review of the documents obtained by the Committee (which included more than 1,700 pages of documents from Imperatis). The agency did procure updated security tools to secure the legacy IT environment (although not all such interactions were handled through this contract, including Cylance) and the new IT environment (Shell/Iaas) that Imperatis built appears to be an improvement over the legacy IT environment. However, there were schedule and cost challenges (as the IG warned) and questions remain as to how OPM will realize the benefits of new Shell/IaaS and at the same time maintain the legacy IT environment in a cost effective way.

Further, OPM has no clear assessment of whether the costs paid to date under this contract—over $45 million—were reasonable, given the lack of competition for the contract. Finally, the long-term plan for securing and modernizing OPM's IT environment remains unclear, especially given ongoing efforts to complete an analysis of alternatives and establish reasonable cost estimates for modernization.

The following is a timeline of events related to the IT Infrastructure Improvement project contract and more details that validate some of the concerns initially identified by the IG.

Office of Personnel Mgmt's Infrastructure Improvement Project – Major IT Business Case at 1 [hereinafter Schlosser Response to Second Interim Status Report].

[1086] Schlosser Response to Second Interim Status Report (Apr. 22, 2016) at 1.

[1087] *Id.* at 3.

Timeline: OPM's IT Infrastructure Improvement Project

- May 10, 2014. Then-OPM CIO Donna Seymour contacts former colleagues (who she knew from her time at the U.S. Maritime Administration (around 2006)) at Imperatis, about the IT security situation at OPM and a potential IT project to address the situation.[1088]

- May 27, 2014. In response to the malicious activity identified in March 2014, OPM executes the "Big Bang" remediation plan. OPM's Director of IT Security Operations, Jeff Wagner and DHS/US-CERT team members provided an unclassified briefing to Imperatis employees.[1089]

- June 16, 2014. Letter contract statement of objectives for Imperatis contract describes activities under the contract in **all four phases** of the IT Infrastructure Improvement project.[1090] The base year of the contract plus options included a period from June 2014 through December 2016. Initially, $18 million was allocated under the letter contract.

- June 22, 2014. DHS/US-CERT issues the OPM Incident Report and makes fourteen recommendations to improve OPM's IT security, including a general recommendation to "redesign their network architecture to incorporate security best practices."[1091]

- October 14, 2014. Solicitation for IT Infrastructure Improvement contract issued as part of the process to definitize the June 2014 Letter contract.[1092]

- November 12, 2014. Imperatis submits a proposal in response to October 14, 2014 solicitation.[1093]

- January 30, 2015. Imperatis contract for OPM's IT Infrastructure Improvement project is definitized.[1094]

- February 2015. OPM FY 2016 Congressional Budget Justification requests $21 million "to implement and sustain agency network upgrades initiated in FY 2014 and security

---

[1088] Email from Donna Seymour, Chief Info Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney and [redacted] Imperatis (May 10, 2014, 9:46 a.m.), Attach. 12 at 001463 (Imperatis Production: Sept. 1, 2015).
[1089] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis Corp. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 8.
[1090] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015). OPM used a DHS contract vehicle, but the former OPM CIO Donna Seymour was designated the contracting officer representative (COR) and thus was responsible for contract performance management. *Id.* at 000011 (designating Ms. Seymour as COR).
[1091] June 2014 OPM Incident Report at HOGR0818-001236.
[1092] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis Corp. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 9.
[1093] Imperatis Proposal Volume I – Statement of Work and Technical, Attach. 5 at 000178 (Imperatis Production: Sept. 1, 2015).
[1094] Imperatis Definitized Contract (Jan. 30, 2015), Attach. 2 at 000040 (Imperatis Production: Sept. 1, 2015).

software maintenance to ensure a stronger, more reliable, and better protected OPM network architecture."[1095]

- March 27, 2015. Imperatis coordinates initial meeting with CyTech and OPM to evaluate CyTech's CyFIR tool for possible use in the new IT Infrastructure (the Shell).[1096]

- March 2015. OIG becomes aware of the IT Infrastructure Improvement Project when the OCIO meet with OIG to discuss the special assessment the OCIO would be collecting from all OPM program offices to partially fund the project.[1097]

- April 2, 2015. CyTech meets with Imperatis and OPM at CyTech office in Manassas.[1098]

- April 15, 2015. OPM notifies US-CERT regarding potential indicators of compromise.[1099]

- April 21-22, 2015. CyTech product demonstration at OPM facilitated by Imperatis.[1100]

- June 15, 2015. The first six month option to continue Shell (phase 2) work is exercised. This option expired December 15, 2015.[1101]

- June 16, 2015. The Committee holds first hearing on the OPM data breach.[1102]

- June 17, 2015. IG McFarland issues Flash Audit Alert to then-Director Archuleta to alert her to "serious concerns" the IG has regarding the OCIO infrastructure improvement project. The IG finds OCIO launched project "without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and costs of the effort required to migrate it to the new environment." The IG also expresses concern that a sole source contract award had been made.[1103]

[1095] U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2016*, at 2 (Feb. 2015), available at: https://www.opm.gov/about-us/budget-performance/budgets/congressional-budget-justification-fy2016.pdf.
[1096] Imperatis Weekly Report (Mar. 30, 2015-Apr. 3, 2015), Attach.6 at 000704 (Imperatis Production: Sept. 1, 2015).
[1097] U.S. Office of Personnel Management, Office of Inspector Gen. *Background Information: OPM Infrastructure Overhaul and Migration Project* (June 17, 2015) (on file with the Committee).
[1098] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Regarding Clarification on Sept. 1, 2015 Production (Sept. 10, 2015) (on file with the Committee).
[1099] AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316-1922-23 (OPM Production: Apr. 29, 2016).
[1100] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Regarding Clarification on Sept. 1, 2015 Production (Sept. 10, 2015) (on file with the Committee).
[1101] Memorandum from the Hon. Beth Cobert, Act. Dir, U.S. Office of Personnel Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Response to Interim Status Report on OPM's Responses to the Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Plan (Report No. 4A-CI-00-15-055)* (Sept. 9, 2015) at 3.
[1102] *OPM Data Breach: Hearing Before the H. Comm. On Oversight and Gov't Reform*, 114th Cong. (June 16, 2015).
[1103] OIG Flash Audit Alert (June 17, 2015).

- June 22, 2015. Then-Director Archuleta responds to IG's Flash Audit Alert regarding the IT Infrastructure Improvement Project. OPM generally disagrees with the recommendations in the Flash Audit Alert, saying there was no time to do a business case and activities associated with the Shell are extensions of existing IT investments.[1104]

- June 24, 2015. The Committee holds a second hearing on the OPM data breach. Then-CIO Donna Seymour testifies "we only contracted for the first two pieces" of the four-phase IT Infrastructure Improvement project. She also says the estimated cost of the initial project phases was $93 million.[1105]

- July 22, 2015. OPM IG McFarland issues a memorandum to Acting Director Cobert on serious concerns regarding the CIO, including CIO's statement to Congress that she was "not aware of a requirement . . . to notify the IG of every project we take on" (in response to a question about the IT Infrastructure Improvement project) and incorrect/misleading information provided by OPM on the sole source contract.[1106]

- August 18, 2015. Committee sends letter to Imperatis requesting information about the IT Infrastructure Improvement project.[1107]

- September 1, 2015. Imperatis provides documents to the Committee in response to August 18 request.[1108]

- September 3, 2015. OIG issues Interim Status Report on the Flash Audit Alert on OPM's IT Infrastructure Improvement project.[1109]

- September 9, 2015. Acting Director Cobert responds to the IG's September 3 Interim Status Report on IT Infrastructure Improvement project.[1110]

- September 17, 2015. Imperatis completes buying cybersecurity tools to secure the legacy IT environment (Tactical Phase 1).[1111]

[1104] Archuleta Response to OIG Flash Audit Alert.
[1105] *Hearing on OPM Data Breach Part II* (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[1106] OIG Serious Concerns Regarding OCIO (July 22, 2015).
[1107] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to Major General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis (Aug. 18, 2015).
[1108] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015).
[1109] OIG Interim Status Report (Sept. 3, 2015).
[1110] Memorandum from the Hon. Beth Cobert, Act. Dir, U.S. Office of Personnel Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Response to Interim Status Report on OPM's Responses to the Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Plan (Report No. 4A-CI-00-15-055)* (Sept. 9, 2015).
[1111] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Questions on Status of the Project (Feb. 12, 2016) (on file with the Committee).

- September 28, 2015. Imperatis completes initial operational capability of the Shell (Phase 2). Imperatis had planned to complete Full Operational Capability early summer 2016. Performance tuning and staff training on new technologies for the Shell were planned to continue through the end of the contract period of performance (December 2016).[1112]

- October 15, 2015. Imperatis provides briefing to Committee staff on their interactions with CyTech and status of the IT Infrastructure Improvement project.

- December 10, 2015. Chairman Chaffetz calls for Seymour to resign for the sixth time citing, in addition to previous concerns, IT Infrastructure Improvement project concerns.[1113]

- January 22, 2016. The White House announces the creation of the NBIB "which will absorb [OPM's] existing Federal Investigative Services (FIS)" and stated the Defense Department "will assume the responsibility for the design, development, security and operation of the background investigations IT systems for the NBIB."[1114]

- February 24, 2016. OPM Acting IG Norbert Vint prepared testimony for a Committee hearing, entitled "OPM Data Breach: Part III" (canceled) and highlighted continuing concerns about the IT Infrastructure Improvement Project and the sole source contract.[1115]

- April 22, 2016. OPM Acting CIO Lisa Schlosser issues a memorandum to the OIG responding to a draft of the Second Interim Status Report on the IT Infrastructure Improvement project and outlining next steps to implement the IG's recommendations.[1116]

- May 6, 2016. Imperatis reports payments from OPM totaling $45.1 million for the period June 16, 2014 through May 6, 2016.[1117]

- May 9, 2016. OPM terminates Imperatis' contract for nonperformance. Imperatis is precluded from public comment due to Non-Disclosure Agreement with OPM.[1118]

[1112] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff Questions on Status of the Project (Feb. 12, 2016) (on file with the Committee).
[1113] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Dec. 10, 2015).
[1114] White House, Press Release, *The Way Forward for Federal Background Investigations* (Jan. 22, 2016), available at: https://www.whitehouse.gov/blog/2016/01/22/way-forward-federal-background-investigations.
[1115] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt. OPM) (cancelled).
[1116] Schlosser Response to Second Interim Status Report (Apr. 22, 2016).
[1117] Email from Impertis to H. Comm. on Oversight & Gov't Reform Majority Staff (June 7, 2016) (on file with the Committee).
[1118] Jack Moore, *Contractor Working on OPM's Cyber Upgrades Suddenly Quits, Citing "Financial Distress,"* NEXTGOV (May 13, 2016), available at: http://www.nextgov.com/cybersecurity/2016/05/contractor-working-opms-cyber-upgrades-suddenly-quits-citing-financial-distress/128301/. Based on information provided to the Committee

- May 18, 2016. The Acting IG issues the Second Interim Status Report on the IT Infrastructure Improvement project noting continuing concern regarding the lack of critical capital project planning practices required by OMB for this project, but also noting some positive actions by OPM.[1119]

- June 2016. Original end date for the first option period for the Imperatis contract.

- December 2016. Original end date for the second option period for the Imperatis contract.

OPM Initiates Contact with Imperatis and Awards Sole Source Contract

On May 10, 2014, then-OPM CIO Donna Seymour initiated contact with two Imperatis employees with whom she had previously worked on a prior IT project at the U.S. Maritime Administration.[1120] She explained that she was looking for assistance to help "straighten out a very messy network with poor security."[1121] Initially, Seymour offered to hire one of these individuals as an OPM employee, but he declined, citing a commitment to his supervisor at Imperatis, and offered instead to provide assistance as an expert consultant.[1122] Seymour said she would investigate potential options for such assistance, adding: "I want/need you on the team."[1123]

OPM and Imperatis continued discussions about the scope of the project and potential costs through late May.[1124] Then on May 27, 2014, Imperatis received an unclassified briefing from Jeff Wagner, OPM's Director of IT Security Operations and members of the US-CERT team regarding the network security incident OPM learned about in March 2014.[1125] In a letter to the Committee, Imperatis told the Committee that this briefing "conveyed an urgent and compelling need for immediate action on both the operational network . . . and for the development of a new, separate and distinct information systems architecture."[1126]

---

the contractor may be experiencing financial difficulty due to an accounting issue for a separate and unrelated contract with another agency.

[1119] OIG Second Interim Status Report on Infrastrcuture Improvement Project (May 18, 2016).

[1120] Email from Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Senior IT Manager and [redacted] Dir. of Strategic Growth, Imperatis (May 10, 2014, 9:46 a.m.), Attach. 12 at 001463 (Imperatis Production: Sept. 1, 2015).

[1121] *Id.*

[1122] Email from Patrick Mulvaney, Senior IT Manager, Imperatis, to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (May 12, 2014, 10:01 a.m.), Attach 12 at 001479 (Imperatis Production: Sept. 1, 2015).

[1123] Email from Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Senior IT Manager, Imperatis (May 12, 2014, 10:10 a.m.), Attach. 12 at 001479 (Imperatis Production: Sept. 1, 2015).

[1124] For example, on May 17, 2014 Imperatis provided labor rates information to Ms. Seymour. *See* Email from [redacted] Dir. of Strategic Growth, Imperatis to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (May 17, 2014, 11:14 a.m.), Attach. 12 at 001482 (Imperatis Production: Sept. 1, 2015).

[1125] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 8.

[1126] *Id.* Imperatis also noted that a decision was made to use a DHS contracting vehicle given their cybersecurity role for the federal government. *Id.*

On June 16, 2014 (just over one month after initially contacting Imperatis), a letter contract award was made to Imperatis.[1127] In the days leading up to this award, Wagner followed up on a phone call with Imperatis. He emailed: "I am looking forward to having you guys come in. My team and I have been working this issue with no funding and limited assistance for four years. It will be awesome to have better opinions and solutions."[1128] Wagner testified to the Committee that "Imperatis was contracted to build out a new environment, and in building out the new environment they were given the initiative to find new technologies and innovation."[1129]

Imperatis and OPM Buy Security Tools to Secure the Legacy IT Environment

Documents obtained by the Committee from Imperatis show a list of ten tools that OPM purchased through the Imperatis contract to secure OPM's legacy network.[1130] Purchases were made beginning in June 2014 up through October 2014.[1131] There were challenges in deploying tools, including delays and technical challenges.[1132] The documents show the time elapsed between the purchase of these tools and completing deployment ranged from almost three to fifteen months.[1133]

The reasons for the extended period of time between purchase and full deployment varied and are not entirely clear from the record. Wagner testified that when OPM rolled out certain tools, such as PIV cards, these deployments "caused certain applications and certain functionalities to break, and it was something that we had to work through."[1134]

Further, in the case of completing the roll out of a tool called ForeScout, the documents show some delay can be attributed to a requirement for "notifications" to applicable unions. ForeScout, which is a tool to manage network access control for devices, was purchased in July

---

[1127] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015); Email from [redacted] Contracting Officer, Dep't of Homeland Sec., to [redacted] Imperatis (June 16, 2014, 3:41 p.m.) at 001556-1598 (Imperatis production: Sept. 1, 2015).

[1128] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Senior IT Manager, Imperatis (June 13, 2014, 1:59 p.m.), Attach. 12 at 001539 (Imperatis Production: Sept. 1, 2015).

[1129] Wagner Tr. at 97.

[1130] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: Oct. 21, 2015) (on file with the Committee).

[1131] *Id.*

[1132] Imperatis told the Committee their role in buying security tools during the Tactical phase of the contract "was limited to acting as a procurement agent to purchase OPM-selected security tools and associated vendor professional services." Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 4. The record indicates that Imperatis while acting as an agent also provided justification for tools and typically did perform some due diligence on these purchases. Email from [redacted] Imperatis, to Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (July 29, 2014, 3:10 p.m.), Attach. 9a at 1160-1161 (Imperatis Production: Sept. 1, 2015) (explaining the benefits of Palo Alto Networks Next Generation Firewalls).

[1133] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: October 21, 2015) (on file with the Committee).

[1134] Wagner Tr. at 72.

2014, but it was not fully deployed until September 2015.[1135] Imperatis stated in a Weekly Report for August 2015 that "approval has not yet been received for Agency-wide memo" and "project sponsor is in notification stage with the Union."[1136] The mitigation strategy for this situation was to "prepare updated project timeline, plan & memo to pilot ForeScout to Non-Union Agency users."[1137]

The documents show there were also situations where Imperatis was not able to perform due diligence because of the expedited nature of a purchase. For example, in July 2014 Imperatis described a risk/challenge area: "OPM's desire to purchase tactical gear without Imperatis being able to perform true due diligence on tool and fit into current 'as is' network."[1138] Part of the proposed mitigation strategy for this challenge was to collect more information from Wagner and request his assistance in setting priorities.[1139] This limitation on due diligence and lack of priorities was identified as a Risk/ Challenge beginning in July 2014 through November 2014 until Imperatis stated "implementations are proceeding and most roadblocks have been cleared."[1140]

Imperatis' Role in Responding to OPM Data Breach Incidents

Imperatis stated to the Committee that they did not perform incident response activities related to the June and July 2015 data breach announcements.[1141] Imperatis said OPM and other OPM contractors were responsible for operations, security, and maintenance of the legacy IT environment. The record does show other contractors with a more significant role in incident response and security of the legacy IT environment.[1142] Imperatis did facilitate meetings with vendors, who played a role in incident response and also did provide "24 man-hours of assistance for security incident response and clean up," according to a Report for the Week of April 27, 2015.[1143] While Imperatis did not perform significant incident response activities, they did have some visibility into the incident response and the IT security challenges related to the data breach incidents announced in 2015.

Imperatis was aware of the March 2014 security incident as demonstrated by documents provided to the Committee. For example, documents show Imperatis was invited to assist OPM

[1135] OPM Tactical Toolset Purchase, Kick-off and Completion Timeframes (Oct. 21, 2015) (Imperatis Supplemental Document Production: October 21, 2015) (on file with the Committee).
[1136] Imperatis Weekly Report (Aug. 3, 2015-Aug. 7, 2015), Attach. 6 at 000942 (Imperatis Production: Sept. 1, 2015).
[1137] *Id.*
[1138] Imperatis Weekly Report (July 8, 2014-July 14, 2014), Attach. 6 at 000342 (Imperatis Production: Sept. 1, 2015).
[1139] *Id.*
[1140] Imperatis Weekly Report (Nov. 10, 2014-Nov. 14, 2014), Attach. 6 at 000478 (Imperatis Production: Sept. 1, 2015);Id, Attach. 6 at 000492 (Imperatis Production: Sept. 1, 2015).
[1141] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 12.
[1142] Saulsbury, an employee of SRA explained his role at OPM saying he had worked at OPM since 2012 as an SRA contractor and worked in network security. He said, SRA provides "supplemental staffing" under a contract to provide a variety of IT management services. Saulsbury Tr. at 8-10.
[1143] Imperatis Weekly Report (Apr. 27, 2015-May 1, 2015), Attach. 6 at 000758 (Imperatis Production: Sept. 1, 2015).

after the primary incident response period for the March 2014 incident.[1144] The Imperatis proposal also stated: "Unfortunately, OPM experienced a recent security incident that occurred because the network was neither set up to easily recognize potential intrusions nor quickly react with the necessary incident response to stop attacks from becoming major data breaches."[1145] Imperatis said by the time of the June and July 2015 OPM breach announcements, the procurement of security tools for OPM's legacy network under the Tactical phase of this project was "nearly 100 % complete."[1146] Imperatis said they did not generally provide incident response services during this period.[1147] However, Imperatis did report that at OPM's request during this period Imperatis "arrange[d] the procurement of Palo Alto firewalls and associated professional services to support the bolstering of network defense around the e-QIP applications" and completed this procurement by July 1, 2015.[1148]

Sole Source, Schedule, and Cost IG Concerns Related to OPM's IT Infrastructure Improvement Contract Validated

Documents and testimony obtained by the Committee show:

OPM Officials Made Statements to Congress that were Inconsistent with the Record.

When the IG raised concerns about OPM making a sole source award for all four phases of the IT Infrastructure Improvement project, OPM officials insisted that a contract award had not been made for the latter two phases of the project (Migration and Clean-Up). Then-CIO Donna Seymour testified before the Committee that "we only contracted for the first two pieces" of this multi-phased project.[1149] Former Director Katherine Archuleta made similar statements before the Committee and elsewhere.[1150]

[1144] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 7-8.
[1145] Imperatis Proposal Volume II – Staffing and Mangement, Attach. 5a at 000233 (Imperatis Production: Sept. 1, 2015).
[1146] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 12.
[1147] *Id.*
[1148] *Id.* Note 1: The e-QIP (Electronic Questionnaire for Investigations Processing System) is used to collect information related to Federal background investigations. On June 29, 2015, OPM shut down the E-QIP system, which was offline until August 4, 2015. Assistant IG Michael Esser said of the shut down, "OPM's official statement on this issue claims that the agency is acting proactively by shutting down the E-QIP system. However, the current security review ordered for this system is a direct reaction to the recent security breaches. In fact, the e-QIP system contains vulnerabilities that OPM knew about, but had failed to correct for years." *Is the OPM Data Breach the Tip of the Iceberg?: Hearing Before* the *Hearing Before Subcomm. on Research & Tech. and Subcomm. on Oversight of the H. Comm. on Science, Space & Tech.*, 114th Cong. (July 8, 2015) (statement of Michael Esser, Assistant Inspector Gen., U.S. Office of Pers. Mgmt.). Note 2: An OPM constructed diagram of how the attacker navigated OPM's system identified [redacted] as one of the affected servers. *See* OPM data breach diagram dated Sept. 1, 2015 at HOGR07264-000947-ur (unredacted version of OPM production: Dec. 22, 2015). An OPM contractor noted in a transcribed interview that he believed [redacted] "related to accessing E-QIP" (Saulsbury Tr. At 76).
[1149] *Hearing OPM Data Breach Part II* (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Management).
[1150] *Hearing OPM Data Breach Part II* (stating "I would like to remind him [the IG] that the contracts for Migration and Cleanup have not yet been awarded."); *Hearing on OPM Information Technology Spending and Data Security*

Later, OPM admitted the contractor did have a role in the latter two phases of the IT Infrastructure Improvement project. On September 3, 2015, Acting Director Cobert supplemented the former Director's response to the IG regarding the sole-source contract and Imperatis' role in the later phases (Migration and Clean up) of the project.[1151] Acting Director Cobert explained that "although the contract contemplates that Imperatis will have work to do in all four phases, not all aspects of the work required by OPM in phases three and four is included in the contract with Imperatis."[1152]

The documents show that while not all work for the project is covered, OPM did in fact make a sole source contract award to Imperatis for work in *all four phases* of OPM's IT Infrastructure Improvement project. Thus, from the beginning, this sole-source award was to cover aspects of work from all four phases of this project. Indeed, the IG pointed out in the June 17 Flash Audit Alert that the original documentation justifying the sole source award covered all four phases of the work (Tactical, Shell, Migration and Clean Up).[1153] The IG also pointed out that in a May 26, 2015 meeting, the former CIO argued in favor of an approach where the same contractor oversaw all four phases of the project.[1154]

The Committee obtained the contract file, which calls into the question the truthfulness of certain statements by OPM officials to Congress. The contract documents outlined in detail the contractor's role in each of the four phases of this project. The Statement of Objectives (SOO) for the June 2014 letter contract states "the work is focused in four primary phases" and then listed tasks that the Contractor was expected to perform under each phase.[1155] For the Migration phase, the SOO stated, "Contractor shall work with OPM to plan for, oversee, and assist in the migration of existing OPM network and business applications and services into the new IT infrastructure."[1156] For the Clean Up phase, the SOO stated, "Contractor shall work with OPM to cleanse all data and applications from unused hardware and shall prepare it to be excessed."[1157] The Statement of Work (SOW) for the contract stated, "[t]he Contractor shall complete work within this SOW in four different phases: Tactical, Shell, Migration, and Clean Up."[1158] The SOW also is similar to the SOO in that the SOW outlines specific contractor tasks in the later two phases of the project.[1159]

(stating "I would like to remind the Inspector General that contracts for the Migration and Cleanup have not yet been awarded.").

[1151] Memorandum from the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Supplement to Response to Flash Audit Alert – U.S. Office of Personnel Mgmt's Infrastructure Improvement Project (Report No. 4A-CI-00-15-055)* (Sept. 3, 2015) [hereinafter Cobert Response (Sept. 3, 2015) to OIG Interim Status Report].

[1152] Cobert Response (Sept. 3, 2015) to OIG Interim Status Report at 1.

[1153] OIG Flash Audit Alert (June 17, 2015) at 5-6.

[1154] *Id.*

[1155] Imperatis Letter Contract Statement of Objectives (June 16, 2014), Attach. 1 at 000007 (Imperatis Production: Sept. 1, 2015).

[1156] *Id.*

[1157] *Id.*

[1158] Imperatis Definitized Contract Statement of Work (Jan. 15, 2015), Attach. 1 at 000077 (Imperatis Production: Sept. 1, 2015).

[1159] *Id. at 81.*

The Committee obtained documents that show the contractor had every expectation that they would be providing services through all four phases of the project. In their November 2014 proposal, the contractor said, "[o]ur response to the SOW directly responds to each of the four phases of the program and describes the ways in which our team has begun fulfilling these requirements to date" and added that their proposal provided "a detailed response and solution to each of the four phases of the Infrastructure Improvement program."[1160] In addition, the contractor outlined in their proposal a five step process with an illustrative diagram for the Migration phase.[1161]

Finally, as the contractor began to perform under the contract, the documents show the contractor was performing tasks related to the later phases of the project. In February 2015, the contractor first identified "stand up of Migration PMO office" as a high risk area and proposed a strategy to mitigate potential risks to include "working closely with ACIOs to ensure IT program managers & application teams are engaged with project plans and a migration schedule is in place."[1162] In early April 2015, the contractor's Weekly Report included a "Migration Process" diagram and discussion of "Migration: Phase 2 options" with pros and cons.[1163] In May 2015, the contractor provided updates on the Migration PMO office saying "Initial engagement happened. There were 2 questions from the application groups."[1164] These activities clearly show the contractor understood the work covered under this contract included tasks related to the Migration phase.[1165]

The IG's Concerns about Schedule Risks Were Validated.

In the June 2015 Flash Audit Alert, the IG raised a concern that OPM had significantly underestimated the time to complete the Migration (Phase 3) of this project and did not consider the complexity and lengthy process to complete this phase.[1166] According to the IG's Alert, OPM estimated the Migration of all of OPM's legacy applications/systems would take eighteen to twenty-four months. Imperatis immediately recognized the schedule challenges and identified schedule risk as a concern in the proposal they submitted. Imperatis's proposal stated: "the duration of the current period of performance is insufficient to accomplish a complete migration into Shell."[1167]

[1160] Imperatis Proposal Volume II – Staffing and Mangement ,Attach. 5a at 000233 (Imperatis Production: Sept. 1, 2015).
[1161] *Id.* at 000222.
[1162] Imperatis Weekly Report (Feb. 16, 2015-Feb. 20, 2015), Attach. 6 at 000649 (Imperatis Production: Sept. 1, 2015).
[1163] Imperatis Weekly Report (Apr. 6, 2015-Apr. 10, 2015), Attach 6 at 000718-20 (Imperatis Production: Sept. 1, 2015).
[1164] Imperatis Weekly Report (May 4, 2015-May 8, 2015), Attach. 6 at 000774 (Imperatis Production: Sept. 1, 2015).
[1165] Imperatis stated in a letter to the Committee that while they were engaged in some role for all four phases of the project, their most significant work related to the Shell – or Phase 2. Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015) at 3.
[1166] OIG Flash Audit Alert (June 17, 2015) at 3.
[1167] Imperatis Proposal Volume I – Statement of Work and Technical, Attach. 5 at 000219 (Imperatis Production: Sept. 1, 2015).

Imperatis also cited, in particular, challenges with applications requiring modernization, including the Federal Investigative Services and Retirement Services.[1168] These applications alone are complex and will take significant time and effort to migrate to modernized solutions.

Two years after the June 2014 award, the tactical phase has been completed, a new IT environment appears to have been delivered (but perhaps not fully tested/trained on), and OPM is still working to inventory and fully scope the alternatives of mitigating or migrating OPM's legacy IT to the new Shell/IaaS. Saulsbury testified to the Committee that he did not work on the Shell, but reported that "Imperatis has some of the infrastructure up and running" and added "Imperatis is starting to train SRA staff on how to operate some of the tools within the shell environment."[1169]

The IG's Concerns about Cost Risks Were Validated.

In the June 2015 Flash Audit Alert, the IG also said there was significant cost "uncertainty" with this project due to the unknown scope of the work required, including a full inventory of OPM's IT assets.[1170] According to Weekly Progress report documents obtained by the Committee, the contractor identified funding for the Shell phase as an area of high risk beginning in February 2015 through at least August 2015.[1171] From March 2015 through April 2015, the contractor updated this high risk area by saying, "still awaiting Mod for additional funding."[1172] In early May 2015 the contractor reported "Mod received. Now discussing additional material funding needed for the rest of FY and FY 2016 through Dec. 15th."[1173] Then in July through August 2015, the contractor update was "need additional funding quickly to ensure no delay in procurement."[1174] The documents show funding for the Shell was a significant ongoing concern.

The uncertainty with respect to total cost of this project has persisted, although OPM now appears to be taking constructive action aimed at improving long term cost estimates. In the June 2015 Flash Audit Alert, the IG reported that OPM had estimated the Tactical (Phase 1) and Shell (Phase 2) portions of the project could cost approximately $93 million, which included $67 million to be collected from major OPM programs as a "special assessment" with little information as to the scope of the project.[1175]

[1168] *Id.*
[1169] Saulsbury Tr. at 11.
[1170] OIG Flash Audit Alert (June 17, 2015) at 3.
[1171] Imperatis Weekly Report (Feb. 23, 2015- Feb. 27, 2015), Attach. 6 at 000658 (Imperatis Production: Sept., 1, 2015); Imperatis Weekly Report (Aug. 10, 2015- Aug. 14, 2015) , Attach. 6 at 000958 (Imperatis Production: Sept. 1, 2015).
[1172] Imperatis Weekly Report (Mar. 23, 2015- Mar. 27, 2015), Attach. 6 at 000700 (Imperatis Production: Sept. 1, 2015); Imperatis Weekly Report (Apr. 20, 2015- Apr. 24, 2015), Attach. 6 at 000746 (Imperatis Production: Sept. 1, 2015).
[1173] Imperatis Weekly Report (Apr. 27, 2015 to May 1, 2015), Attach. 6 at 000760 (Imperatis Production: Sept. 1, 2015).
[1174] Imperatis Weekly Report (July 13, 2015- July 17, 2015), Attach. 6 at 000910 (Imperatis Production: Sept. 1, 2015); Imperatis Weekly Report (Aug. 10, 2015-Aug. 14, 2015), Attach. 6 at 000958 (Imperatis Production: Sept. 1, 2015).
[1175] OIG Flash Audit Alert (June 17, 2015) at 3.

As of late October 2015, OPM reported to the Committee that overall it had spent about $60 million in FY2014 and 2015 for this project.[1176] The contractor has reported being paid a total of $45.1 million for the period of June 16, 2014 through May 6, 2016.[1177]

In May 2016, the IG reported that OPM's FY 2017 Business Case for this project outlined costs already incurred with some "reasonable short-term estimates to finish developing the IaaS portion [Shell]."[1178] However, the IG expressed concerns about the cost estimates for the long term efforts to modernize and migrate to a new IT environment—and called these estimates "unsubstantiated because of the incomplete inventory and technical analysis." At the same time, the IG did acknowledge as positive, OPM efforts to develop cost estimates for modernizing and /or migrating all OPM information systems by leveraging a new application profiling scoring framework.[1179]

In January 2016, the Administration announced the creation of the NBIB and the designation of the Department of Defense (DOD) as responsible for the IT security of background investigation data. This announcement has further complicated efforts to identify a definitive plan to fund IT modernization at OPM given that OPM's background investigation program is being moved to the NBIB and DOD will be responsible for IT security and funding for these functions likely will not be available for modernizing other OPM IT assets.[1180]

The Status and Future Plans for OPM's New IT Environment (Shell/Iaas) are Unclear.

In the June 2015 Flash Audit Alert, the OIG predicted OPM could find itself in a situation where it could be incurring costs to maintain two IT environments (legacy and the Shell). In June 2015, the IG said without a disciplined planning process or a guaranteed funding source in place to complete this likely complex and expensive process, "the agency would be forced to indefinitely support multiple data centers, further stretching already inadequate resources, possibly making both environments less secure, and increasing costs to taxpayers."[1181] The OIG added such a scenario would be inconsistent with the goal of "creating a more secure IT environment at a lower cost."[1182] This appears to now be the case with the creation of the Shell and continued uncertainty about plans and costs for mitigation, modernization and/or migration of OPM's legacy IT environment.

The goal of achieving a more secure environment at lower costs appears to be at risk. In May 2016, the OIG reported that OPM had allocated a "limited amount of funding" to

---

[1176] Email from U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Affairs (Oct. 28, 2015) (on file with the Committee).
[1177] Imperatis Response to H. Comm. on Overisght & Gov't Reform Majority Staff (June 7, 2016) (on file with the Committee).
[1178] OIG Second Interim Status Report on Infrastructure Improvement Project at 7.
[1179] Office of Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI-00-16-037, *Second Interim Status Report on the U.S. Office of Personnel Mgmt's Infrastructure Improvement Project – Major IT Business Case* at 8 (May 18, 2016).
[1180] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (cancelled).
[1181] OIG Flash Audit Alert (June 17, 2015) at 5.
[1182] *Id.*

modernization and migration efforts.[1183] According to the IG, OPM's Business Case for the IT Infrastructure Improvement project allocated only twenty to twenty-five percent of this project's cost for modernization/migration with the remainder allocated to securing and maintaining the legacy and IaaS/Shell environment. The OIG questioned this approach because it does not acknowledge "maintenance cost for the dual environments will not likely remain fixed."[1184] The OIG speculated that as the costs to maintain the legacy environment increase, this could result in limited funding for modernization and migration. Meanwhile, OPM is now currently spending approximately $25 million annually to maintain the IaaS/Shell.[1185]

According to the OIG, OPM is considering a plan to save money by physically moving legacy systems from old data center environments to the new environment.[1186] Such a plan would include keeping the legacy systems in a separate logical environment from Shell/IaaS. It is reasonable to consider such a plan for the purposes of saving money, but as the IG pointed out serious consideration should be given to the security risks of "maintaining security controls in two logical environments indefinitely."[1187]

In sum, OPM's IT Infrastructure Improvement project, which was motivated by the laudable goals of securing the legacy IT environment and creating a more secure lower cost modernized IT environment, fell victim to a flawed contracting and planning approach. Two years after this effort began and after much time and effort to acknowledge and mitigate OIG concerns, OPM is only now making progress toward a disciplined planning and assessment of the alternatives and establishing a reasonable cost estimating process.

[1183] OIG Second Interim Status Report on Infrastructure Improvement Project at 7.
[1184] *Id.*
[1185] *Id.* at 8.
[1186] *Id.* at 7-8.
[1187] *Id.* at 8.

Summary of Investigation

The agency's posture with respect to the Committee's investigation has been consistently uncooperative until the later stages of the investigation, especially as it compares to the level of cooperation from other agencies and contractors who had relevant documents and information.

Committee hearings on the data breaches

On June 16, 2015, the Committee held its first hearing on the OPM data breach, which was entitled "OPM: Data Breach."[1188] The hearing occurred twelve days after OPM publicly announced the breach of personnel records for "approximately four million" current and former federal employees.[1189] The hearing included testimony from witnesses from OPM, the OPM OIG, the OMB, DHS, and DOI. This hearing provided the Committee an opportunity to learn what occurred, based on the information available at that time, but responses from some witnesses increased concerns about the data breach. Following the hearing, Members were invited to a classified briefing on the data breaches.

Twenty days after OPM announced the breach affecting personnel records, the Committee convened a hearing on June 24, 2015, entitled "OPM Data Breach: Part II."[1190] The Committee heard testimony from OPM, the OPM OIG, U.S. Investigations Services, LLC (a former OPM background investigation contractor), and KeyPoint Government Solutions (a current OPM background investigation contractor). During the June 24 hearing, the Committee received an update on the investigation and learned background investigation data also had been compromised, but OPM declined to provide specific information on the number of individuals impacted, citing an ongoing investigation. The Committee also learned more about the OPM data breach discovered in March 2014. Specifically, the Committee heard testimony that "manuals about the servers and environment" had been taken from OPM's network during the incident.[1191] Then-CIO Donna Seymour admitted the "manuals about the servers and the environment" would provide "enough information that [the adversary] could learn about the platform, the infrastructure of [OPM's] system."[1192]

On the same day as the second hearing, then-OPM Director Archuleta sent a letter to Chairman Chaffetz clarifying the number of former and current federal employees' whose personnel records were compromised by saying roughly 4.2 million individuals were impacted and stating an unspecified number of former and current federal employees' background investigation data had been compromised.[1193] It was not until July 9, 2015 that OPM publicly announced the background investigation data of 21.5 million current, former, and prospective

---

[1188] *OPM: Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015).
[1189] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/
[1190] *Hearing on OPM Data Breach: Part II.*
[1191] *Id.*
[1192] *Id.*
[1193] Letter from Katherine Archuleta, Dir., U.S. Office of Personnel Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (June 24, 2015).

federal employees, contractors, and related non-applicants had been compromised.[1194]

Then on July 15, 2015 (just over a month after the breach was first announced), the Committee's Subcommittee on Information Technology and Subcommittee on the Interior held a joint hearing, entitled "Cybersecurity at the U.S. Department of Interior."[1195] Since DOI held OPM personnel records that were stolen in a shared service data center facility, this hearing allowed the Committee to better understand the impact of the breach on DOI, how its systems interacted with those of OPM, and more detail about how the breach occurred. The agency's CIO and Inspector General testified.

In order to learn more about the incidents described at these hearings, the Committee continued its investigation and made multiple requests for information and documents from relevant stakeholders.

Committee request for information regarding identity theft services

On July 21, 2015, Chairman Chaffetz and Ranking Member Cummings sent the first letter to OPM requesting information about: (1) the contract for the identity theft protection services for 4.2 million current and former federal employees' whose personnel record data had been compromised and; (2) OPM's plans to provide identity theft services to the 21.5 million individuals whose background investigation data had been compromised.[1196]

On August 21, 2015, OPM provided an initial response related to the identity theft contract for the 4.2 million personnel records victims to the Committee.[1197] OPM declined to provide detailed information regarding plans for an identity theft services contract for the 21.5 million until a contract had been awarded.

On September 1, 2015, OPM and the Department of Defense (DOD) announced a new identity theft protection and credit monitoring contract award to provide identity theft services to

---

[1194] U.S. Office of Personnel Mgmt., Press Release, *OPM Announced Steps to Protect Federal Workers and others from Cyber Threats* (July 9, 2015) available at: https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/

[1195] *Cybersecurity: The Department of the Interior: Hearing Before the Subcomm. on Info.Tech. and Subcomm. on Interior of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (July 15, 2015).

[1196] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir, U.S. Office of Pers. Mgmt. (July 21, 2015).

[1197] The Committee reviewed the documents OPM provided and confirmed the contract award to Winvale/CSID was not a sole-source award as was originally suggested. However, as the IG later reported there were some contracting irregularities, but it was unclear whether these irregularities would have changed the awardee. On December 2, 2015, the IG completed a Special Review (in response to the Committee's request during the June 24, 2015 hearing) on the $20 million contract to provide credit monitoring and identity protection services to the initial 4.2 million victims of the OPM data breach. The IG's Special Review determined "that in order to meet the OCIO's June 8, 2015, requirements due date, the contracting officer failed to comply with FAR requirements and OPM policies and procedures in awarding the Winvale contract" and then the IG identified five areas of noncompliance. Office of the Inspector Gen., U.S. Office of Pers. Mgmt., 4K-RS-00-16-024, *Special Review of OPM's Award of a Credit Monitoring and Identity Theft Services Contract to Winvale Group LLC and its Subcontractor, CSIdentity*, (Dec. 2, 2014).

the 21.5 million individuals impacted by the background investigation data breach.[1198] After further inquiries to OPM regarding the contract information, OPM deferred to DOD for the details of this contract. The Committee obtained relevant records from DOD on October 20, 2015.[1199]

The DOD award was made under a government-wide contract vehicle established by the General Services Administration (GSA). This contract vehicle provides agencies with access to contractors capable of providing identity monitoring, data breach response, and protection services. This contract vehicle is available to agencies for up to five years and has an estimated value of $500 million. In contrast to the first contract arrangement for the 4.2 million individuals, the September 1, 2015 contract award established a government-wide vehicle for these services so that agencies are not trying to establish a contracting vehicle to provide identity theft services in the middle of incident response. DOD handled the notification process directly for the 21.5 million victims and the initial notification process was completed in December 2015.[1200]

Productions related to the OPM data breaches and CyTech

On July 24, 2015, Chairman Chaffetz and Ranking Member Cummings sent a second letter to OPM requesting information and documents in response to questions about specific details of the data breaches announced in June and July 2015.[1201] The letter covered a range of issues, including information about OPM's relationship with, and the work conducted by, CyTech Services; information on OPM security tools and user credentials for OPM information systems; and additional information related to the data breach.

The request related to CyTech was prompted by a referral from the House Permanent Select Committee on Intelligence (HPSCI) and press reports. On June 15, 2015, the *Wall Street Journal* published a story on the OPM data breaches, alleging that CyTech had discovered the breach during the demonstration of their security tool.[1202] Then on June 23, 2015, just before the Committee's second hearing on the OPM data breaches where the Committee heard testimony about CyTech, the Committee received a memorandum from Rep. Devin Nunes, Chairman of

---

[1198] U.S. Office of Pers. Mgmt., Press Release, *OPM, DOD Announce Identity Theft Protection and Credit Monitoring Contract* (Sept. 1, 2015), available at: https://www.opm.gov/news/releases/2015/09/opm-dod-announce-identity-theft-protection-and-credit-monitoring-contract/.

[1199] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Ray Mabus, Sec., Office of the Sec. of the Navy (Sept. 22, 2015); Letter from R. L. Thomas, Dir., Navy Staff, Dep't of the Navy, Dep't of Defense to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Oct. 20, 2015).

[1200] In the Consolidated Appropriations Act for Fiscal Year 2016, language was including requiring OPM to provide individuals impacted by the OPM data breach with 10 years of identity protection services (versus three years under the Sept. 1, 2015 award) and five million in liability insurance. Jason Miller, *Pay raise, transit benefits parity gives feds optimism for 2016*, FEDERAL NEWS RADIO, Dec. 17, 2016.

[1201] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Director, U.S. Office of Pers. Mgmt. (July 24, 2015).

[1202] Damian Paletta, *Cybersecurity Firm Says It Found Spyware on Government Network in April,* WALL ST. J., June 15, 2015, available at: http://www.wsj.com/articles/firm-tells-of-spyware-discovery-in-government-computers-1434369994.

HPSCI, and Rep. Adam Schiff, HPSCI's Ranking Member, regarding the information from CyTech.[1203]

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

U.S. POLITICS NATIONAL SECURITY

Cybersecurity Firm Says It Found Spyware on Government Network in April

CyTech Services's claim raises questions over how personnel-data theft was discovered

As a result of these events, the Committee sought documents and information to better understand the facts and any role CyTech played at OPM during the 2015 incident response period. Pursuant to this effort, the Committee requested information from OPM about CyTech as part of a broader July 24, 2015 letter to OPM. On August 14, 2015 Chairman Chaffetz also sent an information request to Ben Cotton, Chief Executive Officer of CyTech.[1204] The letter requested all documents and communications between OPM and CyTech, details about the product demonstration that CyTech conducted at OPM in April 2015, and any additional activities conducted by CyTech related to incident response.[1205] CyTech responded to this request on August 19, 2015 by providing documents to Committee staff during a visit to CyTech headquarters in Manassas, Virginia. The Committee also conducted a transcribed interview with Cotton on September 30, 2015.[1206]

While CyTech promptly responded to the Committee's request for information, OPM dragged its feet. OPM's initial response to the Committee's July 24, 2015 letter did not include information in response to questions about CyTech.[1207] On September 25, 2015, OPM made a second production in response to the July 24, 2015 request, producing a nine-page narrative in response to questions posed about CyTech and only one relevant document—more than 175 pages of visitor logs from OPM's Washington, D.C. headquarters for the month of April 2015 that were almost entirely redacted.[1208]

[1203] Letter from the Hon. Devin Nunes, Chairman, and the Hon. Adam Schiff, Ranking Member, H. Permanent Select Committee on Intelligence, to the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 23, 2015).

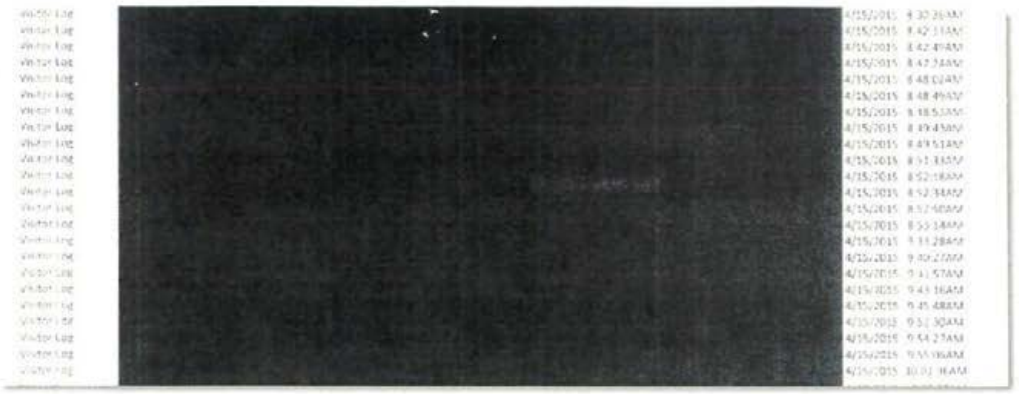
[1204] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Ben Cotton, President & Chief Exec. Officer, CyTech (Aug. 14, 2015) (Ranking Member Cummings did not sign this request).

[1205] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Ben Cotton, President & Chief Exec. Officer, CyTech (Aug. 14, 2015).

[1206] Cotton Transcribed Interview.

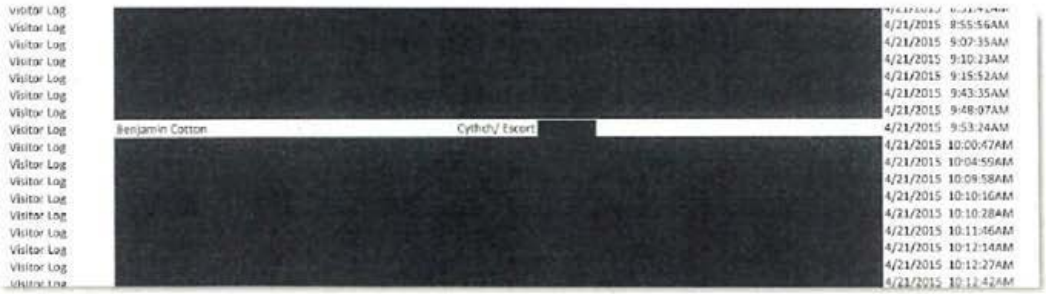
[1207] August 28, 2015 (OPM document production).

[1208] Letter from Jason Levine, Dir. of Cong., Legislative & Intergovernmental Affairs, U.S. Office of Pers.Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 25, 2015) (OPM Production: Sept. 25, 2015); Office of Personnel Management Visitor Log April 1- July 10, 2015 at HOGR724000325-501 (OPM Production, Sept. 25, 2015).



Heavily redacted visitor logs provided by OPM on September 25, 2015

OPM made a third production to the Committee on October 7, 2015 that included a slightly less redacted version of the visitor logs and a corresponding analysis of entries for staff from CyTech, Imperatis, DHS and the FBI.[1209]



On October 28, 2015, OPM made a substantial production of (redacted) documents, made documents available *in camera*, and responded to a September 9, 2015 letter regarding a "deleted drive" on CyTech's CyFIR appliance.[1210] On August 19, 2015, CyTech told Committee staff it had requested the CyFIR appliance be returned multiple times, but it was not returned until August 20, 2015[1211]—one day after Committee investigators visited CyTech offices.

The CyFIR appliance was returned to CyTech sanitized, that is, with all information deleted.[1212] The agency did not provide a copy of the drive's contents to the Committee, despite the fact that there was an ongoing congressional investigation and preservation order in place. The status of the deleted contents of the drive, and whether OPM preserved a copy, was

---

[1209] Office of Personnel Management Visitor Log April 1-July 10, 2015 at HOGR0724-000615-791 (OPM Document Production: Oct. 8, 2015). Additional responsive documents were also made available to the Committee *in-camera* in the OPM liaison office at this time.

[1210] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Sept. 9, 2015).

[1211] Cotton Tr. at 72.

[1212] Email from Brendan Saulsbury, Senior Cyber Security Engineer, SRA to Jonathan Tonda, SRA, U.S. Office of Pers. Mgmt. and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 17, 2015, 1:54 p.m.) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

discussed at length at a January 7, 2016 Committee hearing.[1213] It was not until April 2016, that OPM made a sample of the images collected by CyFIR available for an *in camera* review. OPM had obtained this information for the *in camera* review from US-CERT.

Chairman Chaffetz questions an OPM witness about redactions

Despite Committee requests for information and an August 21, 2015 preservation order, OPM did not preserve all relevant evidence. The preservation order covered all records related to the breach/intrusion, the infrastructure improvement project, cybersecurity, and decisions on implementing the recommendations made by the OIG.[1214]

As a result of documents produced by CyTech, and interviews with CyTech employees, the Committee obtained evidence related to the efforts of other firms involved in the April 2015 incident response activities at OPM, including Cylance, SRA, and Imperatis. Each of these companies was present throughout the incident response period and ultimately provided information useful in understanding the bigger picture of what unfolded before, during, and after the OPM data breaches.

The Committee investigated the role of Cylance

Cylance was first identified during a review of documents provided by CyTech. In an April 24, 2015 email, an employee of Cylance, Chris Coulter, emailed CyTech's CEO to ask: "Would you be able [to] pull this file, want to verify something . . . ."[1215] In a September 28,

---

[1213] *Document Production Status Update: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Jan. 7, 2016) at 1:07.
[1214] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Dir., U.S. Office of Pers. Mgmt. (Aug. 21, 2015).
[1215] E-mail from Chris Coulter, Managing Dir., Cylance, to Benjamin Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 1:54 p.m.) at 1.27 (CyTech Production: Aug. 19, 2015).

2015 briefing to Committee staff, OPM's Director of IT Security Operations, Jeff Wagner, told staff that Cylance executed the quarantine order on OPM's systems in April 2015.

On December 3, 2015, the Committee sent a letter to Cylance inquiring about the activities it conducted at OPM in April 2015 and requested related documents.[1216] Cylance provided thousands of pages of documents on a rolling basis and in a timely manner, and also made available to the Committee a virtual data room with additional pieces of information and evidence.

The Committee subsequently conducted transcribed interviews of two Cylance personnel.[1217] The Committee conducted a transcribed interview with Cylance CEO Stuart McClure on February 4, 2016. On February 12, 2016, the Committee conducted a transcribed interview with Cylance Managing Director of Incident Response and Forensics Chris Coulter. Coulter was heavily involved in providing assistance to OPM with the deployment of Cylance tools.

The Committee investigated the role of SRA

SRA, International, another OPM contractor, provided information that helped inform a more complete picture of the OPM data breach incidents identified in March 2014 and April 2015.[1218] The Committee was able to identify two key SRA employees who provided OPM IT security operations contract support in 2014 and 2015.[1219] The SRA employees provided IT security operations center support under an SRA contract for IT management services and reported to OPM's Director of IT Security Operations, Jeff Wagner.

The Committee contacted one of these SRA employees, Brendan Saulsbury, who responded to questions about his role in the OPM data breach incident response in an informal interview in January 2016. Later, on February 16, 2016, Saulsbury participated in a transcribed interview.[1220] Saulsbury started with SRA in early 2012 and by March 2012 began providing IT security operations support to OPM under an SRA contract. Saulsbury administered various IT security tools and played a key role in the 2014 and 2015 OPM data breach incident response and forensic investigation. The other (now former) SRA employee identified through the Committee's investigation, Jonathan Tonda, began working for OPM as a federal employee in the Fall of 2015. As of May 2016, Saulsbury left SRA and is employed with another organization.

[1216] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to Stuart McClure, Chief Exec. Officer, Cylance (Dec. 3, 2015).
[1217] McClure Tr.; Coulter Tr.
[1218] SRA International has combined with the North American Public Sector business of CSC to form SRA in the fall of 2015. *See* CSC, Press Release, *CSC to Combine Government Services Unit with SRA Upon Separation from CSC; Combination Will Create Leading Pure-Play Government I.T. Business in the U.S.* (Aug. 31, 2015).
[1219] E-mail from Brendan Saulsbury, Contractor for OPM IT Security Operations, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 11, 2015, 11:44 p.m.) (CyTech Production Aug. 19, 2015).
[1220] Saulsbury Tr.

The Committee Investigated OPM's IT Infrastructure Improvement Project and the Contract Awardee Imperatis

On June 17, 2015, OPM's IG issued a Flash Audit Alert to then-Director Katherine Archuleta regarding OPM's contract award to Imperatis for the IT Infrastructure Improvement project.[1221] This contract was awarded in June 2014 as part of OPM's response to the data breach discovered in March 2014. The Committee requested follow up information from the IG and raised further questions about this contract, based on the Flash Audit Alert during the June 24, 2015 hearing.[1222] The Flash Audit Alert also led the Committee to review the Imperatis contract and its role in activities at OPM in April/May 2015 related to the data breach incident response. As part of Imperatis activities for the Tactical (Phase 1) portion of the IT Infrastructure Improvement project, Imperatis coordinated meetings with CyTech and OPM and ultimately CyTech's demonstration of its CyFIR tool at OPM on April 21, 2015. The CEO of CyTech identified key Imperatis personnel onsite for demonstration, which assisted the investigation.

Chairman Chaffetz sent an August 18, 2015 letter to Imperatis requesting documents and communications related to CyTech and the IG's Flash Audit Alert.[1223] On September 1, 2015, Imperatis responded to the Chairman's request and produced over 1,700 pages on the IT Infrastructure Improvement project contract, including information on pre-contract communications between OPM and Imperatis employees, the security tools tested and deployed, and contract performance.[1224] In addition, Imperatis provided a briefing to Committee staff on October 15, 2015, explaining its role in scheduling and participating in the CyTech demonstration. Finally, Imperatis responded to supplemental requests by majority staff on contract developments and clarifications on its document production.

Document productions by Department of Homeland Security

On August 19, 2015, Chairman Chaffetz sent a letter to US-CERT requesting information and documents related to its role in assisting OPM with incident response and the forensics investigation of the data breaches identified in March 2014 and Spring 2015.[1225] US-CERT was reluctant to provide documents directly and quickly because US-CERT expressed a preference that OPM provide all US-CERT documents directly to the Committee due to its view that the documents were similar to a client's information. Regardless of this view, it is US-CERT's responsibility to fully respond in a timely manner to congressional information requests. The Committee ultimately received a production of over 350 pages from US-CERT on December 11, 2015 – nearly four months after the initial request.[1226] The delay in receiving this information

[1221] OIG Flash Audit Alert (June 17, 2015).
[1222] *OPM Data Breach: Part II* (June 24, 2015).
[1223] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to Major General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis (Aug. 18, 2015).
[1224] Letter from Maj. General (ret.) Mastin Robeson, President & Chief Exec. Officer, Imperatis to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 1, 2015).
[1225] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Ann Barron-DiCamillo, Dir., U.S. Comp. Emergency Readiness Team, U.S. Dep't of Homeland Sec. (Aug. 19, 2015).
[1226] Letter from M. Tia Johnson, Ass't Sec't for Legislative Affairs, U.S. Dep't. of Homeland Sec. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Dec. 11, 2015).

could have been avoided had OPM and US-CERT been more timely and responsive to Committee requests.

Unnecessary delays, restrictions, redactions and a congressional subpoena

From July 2015 until early spring of 2016, OPM provided sluggish and incomplete responses to requests, offering only *in-camera* review of certain documents, and documents that were often riddled with redactions. Further, OPM finally produced key documents with limited redactions to the Committee just a few days before the Committee conducted a transcribed interview with OPM's Director of IT Security Operations, Jeff Wagner on February 18, 2016.[1227]

Unnecessary delays

Of the multiple information requests sent to OPM prior to the February 3, 2016, subpoena, not a single one was answered completely within the requested timeframe. This lack of cooperation slowed the Committee's investigation and resulted in the Committee having to make multiple requests to other stakeholders.

For example, on August 18, 2015, Chairman Chaffetz sent another letter to OPM regarding the "stolen manuals" issue and requested a response by September 1, 2015.[1228] The letter referenced June 24, 2015 hearing testimony from then-CIO Donna Seymour responding to the Chairman's questions about the exfiltration of security documents and manuals related to OPM's network.[1229] The letter requested documents and communications about the incident and the information that was stolen.[1230]

When OPM responded on September 18, 2015, the response contained significant redactions.[1231] In fact, it was not until January 12, 2016 (nearly five months after the initial letter was sent) and after a congressional hearing where Members of the Committee expressed frustration about the redactions, that OPM made the unredacted documents available *in camera*. OPM finally produced these documents to the Committee without redactions on February 16, 2016. The stolen manual production was critical to understanding more about the data breach discovered in March 2014.

Unnecessary redactions

The agency routinely provided the Committee with documents containing unnecessary redactions. In addition to the aforementioned visitor logs that were redacted to the point of

---

[1227] Wagner Tr. at 23.
[1228] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Aug. 18, 2015).
[1229] *Id.*
[1230] *Id.*
[1231] Letter from Jason Levine, Dir., Cong., Legislative & Intergovernmental Affairs, Office of Pers. Mgmt., to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 18, 2015).

initially being useless,[1232] the agency redacted the name of OPM press officials in some cases.[1233] There is no valid basis for OPM to redact the name of its press officials, especially given their very public role in communicating with the press and public.

In another example, OPM redacted the name of the contracting officer who was managing the first contract for the identity protection services for breach victims.[1234] The agency redacted the name of the officer despite the fact that his name was publicly available on a now archived Fed BizOps website page.[1235] Further, the Committee requested the *curriculum vitae* of Jeff Wagner, OPM's Director of Security Operations, in its July 24, 2015, letter to OPM.[1236] When OPM responded to the request over a month letter, OPM redacted Wagner's name.[1237]

Director of the Office of Congressional Affairs Jason Levine testifies before the Committee

[1232] OPM redacted virtually every name on the visitor logs it provided the Committee pursuant to the July 24, 2015 letter's second request.
[1233] E-mail from [redacted], to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt (June 12, 2015, 1:50 p.m.), at HOGR020316-000211 (OPM Production Feb. 16, 2016).
[1234] Winvale Contract (June 2, 2015) at 028 (OPM Production: Aug. 21, 2015).
[1235] Solicitation Number: OPM3215T0019 (May 28, 2015) available at: https://www.fbo.gov/index?s=opportunity&mode=form&id=ebef7df6fb8783dbc59c977962833760&tab=core&tabmode=list&print_preview=1.
[1236] Letter from the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (July 24, 2015).
[1237] Letter from Jason Levine, Dir., Cong., Legislative & Intergovernmental Affairs, U.S. Office of Pers. Mgmt., to the Hon. Jason Chaffetz, Chairman, and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2015), (OPM Production: Aug. 28, 2015).

Subpoena issued to OPM

In a January 7, 2016 hearing before the Committee, Jason Levine, Director of the Office of Congressional, Legislative and Intergovernmental Affairs at OPM testified that "OPM has worked tirelessly . . . to respond to numerous congressional inquiries regarding the incidents" and that "OPM has made every effort to work in good faith to respond to multiple congressional oversight requests, including document productions."[1238]

Seven months after the Committee's first request to OPM for information, the Committee issued a subpoena on February 3, 2016, to compel the agency to produce unredacted documents on a permanent basis.[1239] As outlined above, the Committee invested significant time and effort in attempting to extract documents and relevant information from OPM in the months leading up to the February 3, 2016 subpoena.[1240] While OPM did eventually produce requested documents without redactions directly to the Committee, it was only after multiple rounds of productions and significant time and effort to extract these documents from OPM. The fact is that OPM failed to fully cooperate with this investigation until a subpoena triggered greater cooperation.

In contrast to OPM, other relevant stakeholders contacted by the Committee were cooperative and responsive to the Committee's requests. The Committee received documents from contractors and other relevant entities that it would receive from OPM months later. For example, CyTech provided documents to the Committee on August 19, 2015, that included email conversations between OPM's Director of Security Operations, Jeff Wagner, and CyTech CEO Ben Cotton regarding the *Wall Street Journal* story on CyTech.[1241] The agency produced this same document in February 2016 (after the subpoena had been issued).[1242] In another example, CyTech produced an email in August 2015 that led the Committee to investigate Cylance's role in the incident response activities in April 2015 that OPM only produced in February 2016.[1243]

[1238] *Document Production Status Update: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong., (Jan. 7, 2016) (Statement of Jason K. Levine, Dir., Office of Cong.l, Legislative, and Intergovernmental Affairs, U.S. Office of Pers. Mgmt.).

[1239] Subpoena from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to Beth Cobert, Acting Dir., U.S. Office of Personnel Mgmt., (Feb. 3, 2016).

[1240] *Id.*

[1241] Cotton Tr., Ex. 10 (Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 12, 2015)).

[1242] Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 12, 2015, 1:07 p.m.) at HOGR020316-000205 (OPM Production: Feb. 16, 2016).

[1243] Cotton Tr., Ex. 5 (Email from Chris Coulter, Managing Dir., Cylance, to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015)); Email from Chris Coulter, Managing Dir., Cylance, to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 5:54 p.m.) at HOGR020316-000010 (OPM Production: Feb. 16, 2016).

Conclusion

The devastating consequences of OPM cyberattacks discovered in 2014 and 2015 will be felt by the country for decades to come. The key question now before the country is how will we respond? Federal agencies, including OPM, must remain vigilant in protecting the information of hundreds of millions of Americans and in an environment where a single vulnerability is all a sophisticated actor needs to steal or alter Americans' information, the identities of average Americans, and profoundly damage the interests of U.S. national security.

The longstanding inability of OPM to adequately implement sometimes basic, but necessary security measures, despite years of warnings from its Inspector General, represents a failure of culture and leadership, not technology. However, the Committee remains hopeful that OPM, under the new leadership of Acting Director Beth Cobert, is in the process of remedying decades of mismanagement.

In late June 2016, OPM reported to the Committee that over the past year "OPM has taken significant steps to enhance its cybersecurity posture, protect individuals who had their data stolen in the incidents last summer, and reestablish confidence in its ability to deliver on OPM's core missions."[1244] OPM reports such steps include:

- Completing deployment of two-factor Strong Authentication for all users, which provides a strong barrier to OPM's networks from individuals that should not have access;
- Implementing a continuous monitoring program for all IT systems;
- Creating and hiring a cybersecurity advisor position that reports to the Director;
- Establishing an agency-wide centralized IT security workforce under a newly hired Chief Information Security Officer (CISO);
- Modifying the OPM network to limit remote access to exclusively government-owned computers;
- Deploying new cybersecurity tools, including software that prevents malicious programs and viruses on our networks;
- Implementing a Data Loss Prevention System which automatically stops sensitive information, such as social security numbers from leaving the network unless authorized; and
- Enhancing cybersecurity awareness training with emphasis on Phishing emails and other user based social engineering attacks.[1245]

OPM also reports that it has taken steps to improve its cybersecurity capabilities, many of which are part of the President's Cybersecurity National Action Plan. In particular, OPM reports being one of the first agencies to fully implement DHS' Continuous Diagnostics and Mitigation (CDM) program, and that it is targeted to complete its deployment by the end of summer 2016. OPM reports that CDM will allow OPM to communicate with DHS more rapidly and effectively

[1244] Email from Jason Levine, Dir., Office of Cong., Legislative, & Intergovernmental Affairs, U.S. Office of Pers. Mgmt., to H. Comm. on Oversight & Gov't Reform Staff (June 21, 2016, 6:54 p.m.) (on file with the Committee).
[1245] *Id.*

during cybersecurity incidents. In addition, OPM has also completed the implementation of the latest release of Einstein – Release 3a, which is a DHS IT defensive system that collects, detects, and prevents many cyber threats and potential cyber-attacks before they can reach OPM networks and its users.[1246]

But questions remain as to the state and utility of OPM's new information technology infrastructure. How will the newly established National Background Investigations Bureau (NBIB) impact the new IT infrastructure that OPM has built, and that was designed for the Federal Investigative Service which will now belong to the DOD-administered NBIB? Such questions linger as OPM continues to spend tens of millions to maintain and operate both their existing legacy IT environment and the new IT infrastructure. Only time will tell if OPM is able to sufficiently respond to the call for the agency to address its information security shortcomings and IT challenges, especially given the reality that federal CIOs have an average tenure of only two years.[1247]

As Representative Will Hurd, Chairman of the Information Technology subcommittee, stated during the first hearing, the data breach at OPM this "is just another example of the undeniable fact that America is under constant attack. It is not bombs dropping or missiles launching; it is the constant stream of cyber weapons aimed at our data."[1248] OPM and all federal agencies must overcome the unique challenges that each faces with regard to their information environments. Every American must have the confidence that the data they continue to entrust with the federal government will be protected. Agency leadership and their CIOs must be the ones to restore the public trust following the events that transpired at OPM.

[1246] Id.

[1247] Gov't Accountability Office, GAO-11-634, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (Oct. 2011).

[1248] *OPM Data Breach: Hearing Before H. Comm. on Oversight and Gov't Reform*, 114th Cong. (June 16, 2015) (Statement of Rep. Will Hurd).

Appendix: Cyber security Spending at OPM (Fiscal Years 2012-2015)

Table 1. Federal cybersecurity spending by agency (in millions) for FY2015[1249]

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shaping the Cybersecurity Environment	Total
Department of Agriculture	$39	$39	$5	$83
Department of Commerce	$43	$79	$71	$194
Department of Education	$8	$18	$0	$27
Department of Energy	$130	$105	$68	$303
Department of Justice	$291	$131	$35	$456
Department of Labor	$6	$12	$4	$22
Department of State	$102	$73	$25	$200
Department of Transportation	$41	$49	$5	$95
Department of Veterans Affairs	$96	$89	$25	$210
Department of the Interior	$13	$20	$28	$61
Department of the Treasury	$159	$96	$16	$271
Department of Defense	$3,200	$1,100	$4,800	$9,100
Department of Health & Human Services	$71	$132	$17	$220
Department of Homeland Security	$316	$771	$225	$1,313
Department of Housing & Urban Development	$7	$8	$1	$15
Environmental Protection Agency	$2	$12	$3	$17
General Services Administration	$16	$24	$6	$46
International Assistance Programs	$8	$8	$5	$22
National Science Foundation	$3	$6	$206	$215
National Aeronautics & Space Administration	$30	$54	$23	$107
Nuclear Regulatory Commission	$8	$13	$3	$25
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$2	$8	$0	$10
Social Security Administration	$51	$38	$2	$91
Total Cybersecurity Spending	**$4,646**	**$2,887**	**$5,577**	**$13,110**

NOTE: Due to rounding, categories may not sum to the total

[1249] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2015 Annual Report to Congress: Federal Information Security Management Act* (Mar. 18, 2016), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf.

Table 2. Federal cybersecurity spending by agency (in millions) for FY2014[1250]

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shaping the Cybersecurity Environment	Total
Department of Agriculture	$40	$46	$2	$88
Department of Commerce	$56	$83	$74	$213
Department of Education	$11	$20	$1	$32
Department of Energy	$108	$78	$71	$257
Department of Justice	$102	$433	$44	$579
Department of Labor	$13	$3	$1	$17
Department of State	$55	$54	$5	$114
Department of Transportation	$42	$44	$5	$91
Department of Veterans Affairs	$13	$131	$9	$153
Department of the Interior	$17	$30	$1	$48
Department of the Treasury	$122	$68	$10	$200
Department of Defense	$2,552	$1,225	$5,178	$8,955
Department of Health & Human Services	$54	$91	$25	$170
Department of Homeland Security	$473	$722	$148	$1,343
Department of Housing & Urban Development	$6	$8	$0	$14
Environmental Protection Agency	$1	$6	$0	$7
General Services Administration	$27	$16	$10	$53
International Assistance Programs	$9	$4	$3	$16
National Science Foundation	$3	$6	$154	$163
National Aeronautics & Space Administration	$35	$48	$19	$102
Nuclear Regulatory Commission	$4	$12	$3	$19
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$1	$4	$0	$5
Social Security Administration	$46	$11	$2	$59
Total Cybersecurity Spending	**$3,792**	**$3,148**	**$5,765**	**$12,705**

NOTE: Due to rounding, categories may not sum to the total

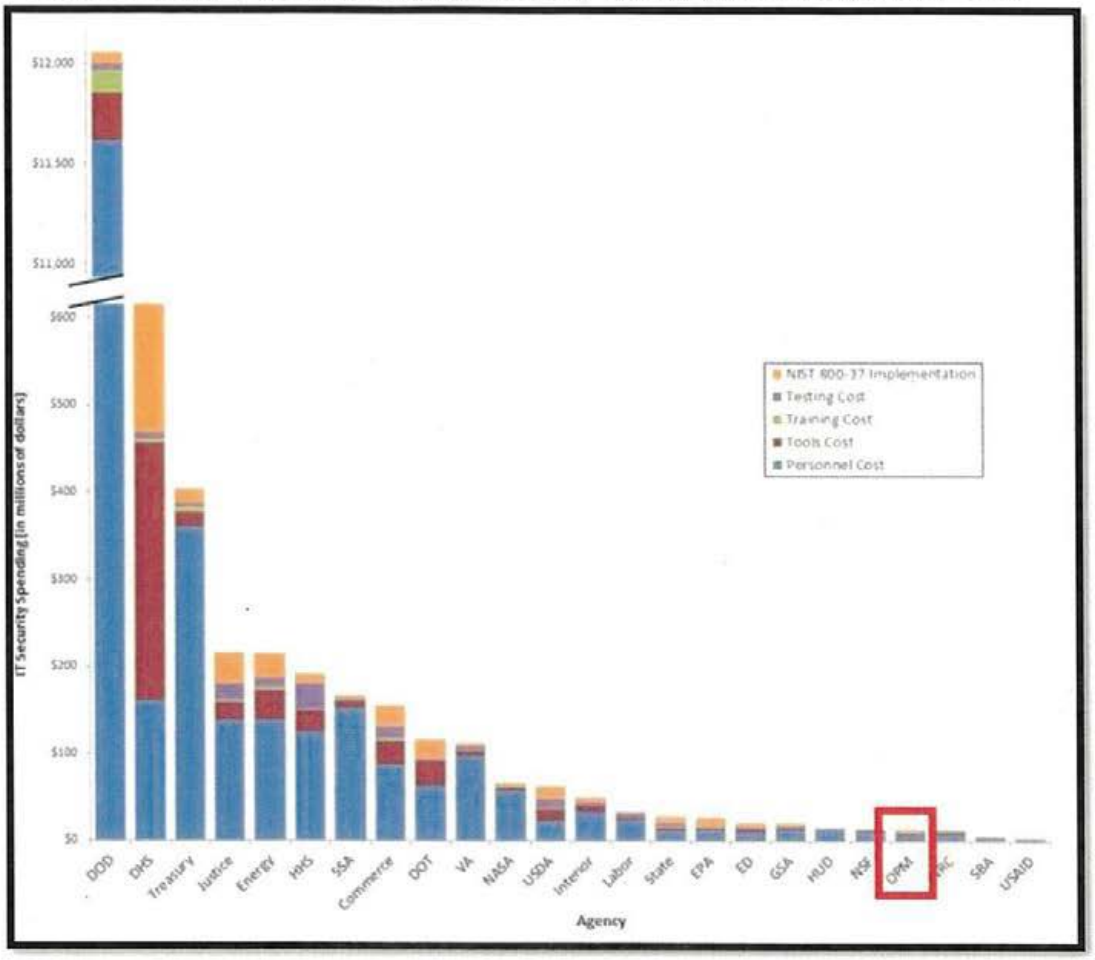
[1250] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014Annual Report to Congress: Federal Information Security Management Act* 83 (Feb. 27, 2015), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

Table 3. Federal cybersecurity spending by agency (in millions) for FY2013[1251]

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shape the Cybersecurity Environment	Total
Dept. of Agriculture	$39	$23	$1	$63
Dept. of Commerce	$47	$74	$42	$163
Dept. of Education	$11	$11	$0	$22
Dept. of Energy	$112	$69	$37	$218
Dept. of Justice	$105	$335	$6	$446
Dept. of Labor	$5	$9	$9	$23
Dept. of State	$51	$30	$5	$86
Dept. of Transportation	$44	$48	$5	$96
Dept. of Veterans Affairs	$11	$102	$7	$121
Dept. of the Interior	$13	$24	$1	$38
Dept. of the Treasury	$146	$109	$13	$268
Dept. of Defense	$2,471	$1,055	$3,580	$7,106
Dept. of Health & Human Services	$44	$111	$26	$181
Dept. of Homeland Security	$369	$590	$150	$1,109
Dept. of Housing & Urban Development	$4	$7	$0	$12
Environmental Protection Agency	$1	$19	$0	$20
General Services Administration	$28	$10	$8	$46
International Assistance Programs	$8	$7	$7	$22
National Science Foundation	$3	$6	$141	$150
NASA	$27	$40	$19	$86
Nuclear Regulatory Commission	$4	$10	$3	$17
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$1	$4	$0	$5
Social Security Administration	$27	$11	$2	$40
Total Information Security Spending	**$3,575**	**$2,707**	**$4,063**	**$10,344**

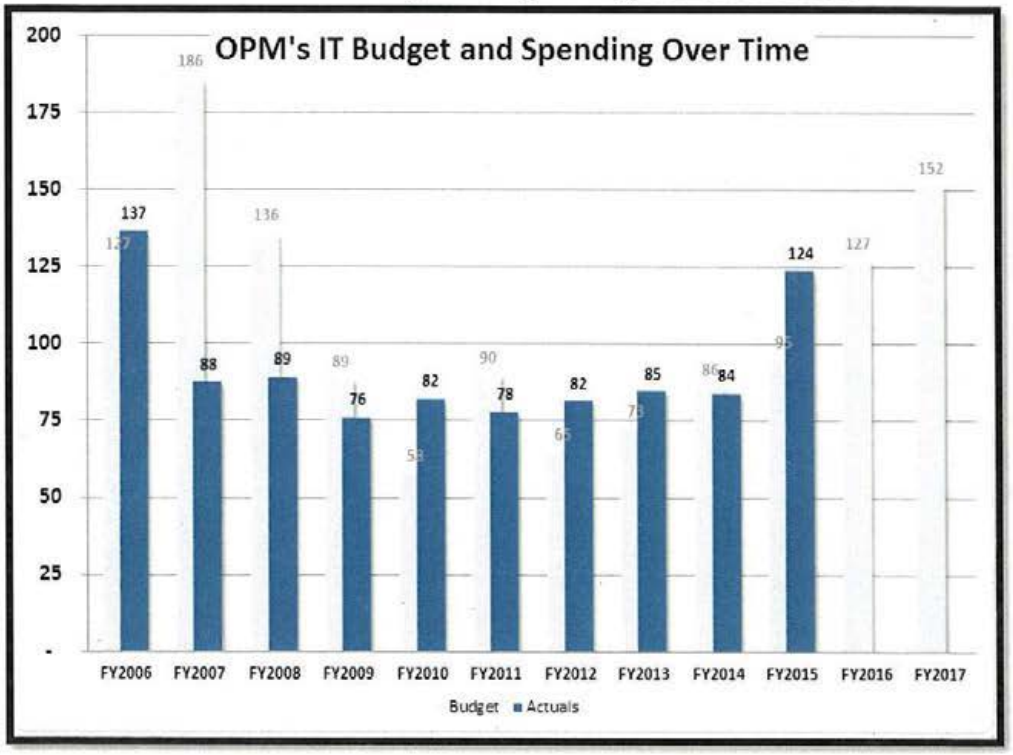
[1251] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2013Annual Report to Congress: Federal Information Security Management Act* 65 (May 1, 2014), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf.

Table 4. Federal cybersecurity spending by agency (in millions) for FY 2012[1252]



[1252] Office of Mgmt. & Budget, Exec. Office of the President, *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* (Mar. 2013), https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

Table 5. OPM IT Budget and Spending, FY2006-FY2017[1253]



[1253] U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2016*, at 2 (Feb. 2015), https://www.opm.gov/about-us/budget-performance/budgets/congressional-budget-justification-fy2016.pdf.. Cybersecurity is one line item in OPM's total IT budget. The amounts requested for IT spending overall, and the amounts appropriated, are shown in the Appendix. In addition, overall funding spikes in 2007 and 2008 are attributed to a transfer from the Trust Fund for retirement modernization. *See* U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2007* (Feb. 6, 2006), https://www.opm.gov/about-us/budget-performance/budgets/2007-budget.pdf; U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2008* (Feb. 5, 2007), https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf.